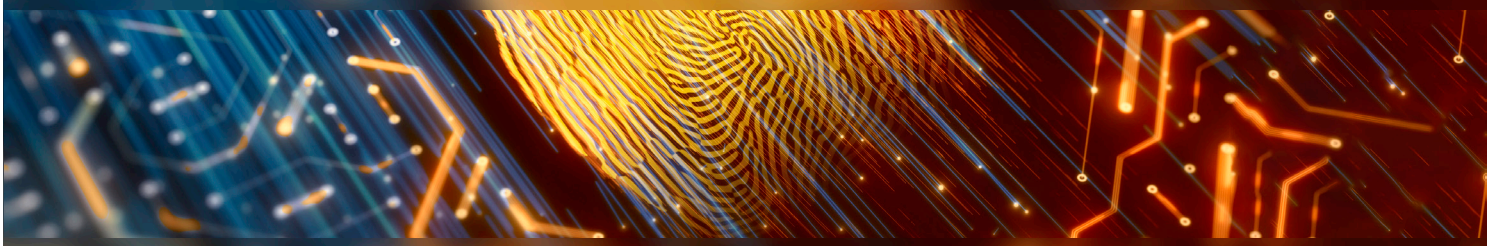
CLIFFORD

CHANCE



RANSOMWARE: PREVENTION & RESPONSE

DECEMBER 2020

CONTENTS

1. INTRODUCTION

Ransomware attacks have drastically increased and become more sophisticated in the wake of the COVID-19 pandemic. Even before this uptick, cybersecurity professionals had predicted global damages from ransomware to reach USD 20 billion in 2021, over 50 times higher than the cost in 2015. In a survey conducted in early 2020 of 5,000 IT managers employed by a range of organizations across 26 countries, over half reported being the target of a ransomware attack—and 75% reported that attackers were successfully able to infect their systems.

In addition to costing companies millions of dollars, ransomware attacks have also become a significant source of regulatory and reputational risk. As privacy and data security increasingly penetrate the global zeitgeist, reports of ransomware attacks have become regular fixtures in international news publications across the globe.

This publication aims to help companies understand and address the risk of a ransomware attack. It provides guidance on how to prevent and prepare for ransomware attacks, what to do if and when a company is the victim of such an attack, important legal considerations from different key jurisdictions, and describes how Clifford Chance can help.

Spotlight: First Ransomware-Related Death in 2020

Ransomware doesn't just threaten a company's operational and financial health—the ripple effects of ransomware attacks can have life-or-death consequences. In fall 2020, a ransomware attack caused the failure of IT systems at the Dusseldorf University Clinic, a major hospital affiliated with Heinrich Heine University. The ransomware attack was directed toward the university, but it infected the hospital's IT systems, forcing staffers to redirect emergency patients as the clinic worked to restore operations. Dusseldorf police eventually established contact with the hackers, who withdrew their ransom demand and provided a digital key to decrypt the data when they learned the attack was affecting patients. But the damage had already been done—on September 17, a woman who needed urgent care died en route to another hospital, after being redirected as a result of the attack.

2. ANATOMY OF AN ATTACK

A ransomware attack combines malicious software (malware) with extortion. Attackers infect devices or systems with malware to block access, demanding payment to restore access and sometimes to avoid dissemination of exfiltrated data.

Stage 1: Infection

A ransomware attack begins with malware. Attackers exploit vulnerabilities in order to gain access to a device or system. This can be accomplished in a number of different ways. In some cases, attackers can crack weak security defenses and gain direct access to devices or systems, remotely installing malware. Other attackers may exploit system software vulnerabilities to find backdoors into a targeted system.

One means of attack that has become increasingly popular among ransomware groups is spear phishing. Spear phishing involves targeting key employees—such as IT staff—and using social engineering tactics to acquire credentials or access. For example, attackers may send a targeted email purporting to be a family member attaching a picture file with malicious code. Or they may masquerade as a senior executive needing to "reset" their password due to a security incident. In these instances, attackers will often study their targets in advance to increase the chance of success.

Stage 2: Attack

Once malware has been installed, the actual ransomware attack proceeds. Sometimes malware will stay dormant for a period to avoid detection. Eventually, however, the malware goes to work, crippling the system. In addition, ransomware perpetrators have increasingly begun to exfiltrate data prior to issuing an extortion demand, and then seek payment as a condition for returning (and not further disseminating) that data.

Stage 3: Extort

Once the device or system becomes fully disrupted, the attackers will make their demands. Most of the time this will be a demand for payment. Typically, these demands seek payment in untraceable cryptocurrency (*e.g.,* Bitcoin).

Stage 4: Spread

Ransomware attackers have become increasingly organized, forming "groups" and conducting repeated attacks over a sustained period of time. Accordingly, ransomware attackers will often look to leverage successful attacks to identify new victims—or continue exploiting existing victims. For example, malware can be designed to lay dormant before it is activated again months or years later. Attackers can also use their access into one company to attack clients or service providers of that first victim.

Types of Ransomware

"Locker" ransomware attacks directly block access to a device or system. In such an attack, underlying data remains intact.

"Crypto" ransomware attacks encrypt data, rendering it unreadable. Devices or systems remain accessible, but data cannot be processed without a decryption key.

3. PREVENTION & PREPARATION

The best way to defend against ransomware is to prevent the attack in the first place, and to be prepared to respond if an attack does occur.

Strong Cybersecurity Measures

Most companies are required by law to have reasonable cybersecurity measures in place to protect personal information. Such measures should help prevent ransomware infections. These measures include:

- Network security (*e.g.,* firewalls, antivirus software, and network traffic monitoring) to prevent and identify intrusions and suspicious activity;
- Software patch management to eliminate software vulnerabilities;
- Remote access security measures (*e.g.,* VPNs, multifactor authentication) to ensure secure work-from-home capability; and
- Segmented networks to limit spread of malware.

Training

Training is critical to preventing attacks. As discussed in Part 2, one of the most common means of introducing malware into a system is through spear phishing. As attackers become more sophisticated, it is more important than ever for companies to train all staff—and in particular key employees such as IT, finance, and human resources personnel—to identify potential attacks. This includes "testing" employees by sending simulated spear phishing emails, and training employees on the measures they should take if they suspect an attack, such as immediately reporting the incident and isolating and segmenting devices suspected to be infected.

Spotlight: Attackers Increase Pressure to Pay by Threatening Publication

In recent years, companies have become more sophisticated in their IT security, implementing protective measures against ransomware attacks such as system backups and rollback technology. In response to this increasing resistance, the Maze ransomware group introduced a new extortion technique in 2019—actually exfiltrating data and threatening to publish it. This technique is particularly devastating for companies that possess sensitive personal data for customers, clients, or other third parties. Since this technique was introduced, a number of major ransomware groups have also incorporated the tactic into their playbooks.

Backup & Disaster Recovery

All companies should have an established backup and disaster recovery policy. Where complete system backups are not feasible, backups should be maintained for business-critical data and processes. Backups should be segmented from primary systems to prevent any malware from spreading to such backups.

Get Down with IOCs

An Indicator of Compromise (IOC) is a piece of forensic computer data that identifies potential malicious activity on a system or device. These could be things like system log entries, network traffic patterns, or IP addresses of known attackers. Law enforcement, IT professionals, and others use IOCs to detect and prevent cyber attacks.

Incident Response Plans

In addition to disaster recovery, companies should have in place robust incident response plans. The specific elements that should be part of such plans are discussed below, but it is important to understand that such policies and procedures must be well established before an incident occurs. Relevant personnel should be trained on the incident response plan and disaster recovery procedures. Tabletop exercises will help ensure that procedures are effective and efficient, so that staff will be prepared in the event of an actual incident.

4. RESPONDING TO AN ATTACK

Ransomware attacks can happen to even the most well-protected company, so companies must be prepared to quickly mitigate and remediate any damage.

Immediate Response

A robust incident response plan will help companies prioritize key actions they will need to take immediately after discovering a ransomware attack. These include:

- Establishing an internal steering group to oversee incident response;
- Segregating and isolating the malware infection to limit its spread;
- Developing an external communication strategy to control information flow;
- Establishing internal communication protocols to ensure staff are informed;
- Implementing backup and disaster recovery plans to permit business to continue (if appropriate and safe to do so);
- Engaging key external advisors, including legal and forensic advisors;
- Taking care to maximize legal privilege protection over internal communications and (where possible) the work of forensic teams;
- Determining regulatory reporting obligations and timelines; and
- Examining contractual notification obligations to key counterparties.

Many of these elements can be prepared in advance (*e.g.,* template press releases, approved pre-selected vendors).

Payment

One of the obvious immediate issues victims of a ransomware attack must consider is whether to pay the ransom. There is no "correct" answer to this question, but companies should consider:

- Whether there are alternatives to payment (*e.g.,* backups);
- Legal ramifications of payment (*e.g.,* sanctions law in the United States, see Part 5); and
- The company's specific reputational concerns.

Notably, research has found that the average cost to a victim of a ransomware attack almost doubles when ransom is paid. And while most companies who pay are able to recover their data, payment of a ransom does not excuse regulatory notification obligations, nor does it guarantee that exfiltrated data will not be further disseminated.

Cyberinsurance

As ransomware and other cyber attacks become more prevalent, cyberinsurance has become crucial. Just as with any other insurance policy, however, coverage will vary. For example, not all policies cover actual ransom payments. Understanding these policies in advance will help ensure companies are not caught by surprise if and when a ransomware attack does occur.

Investigation & Remediation

While some of the most critical work in responding to a ransomware attack will occur in the days immediately following the incident, much of the work will continue for weeks and months following the attack, in the investigation and remediation phase.

Key considerations for this process include:

- Analyzing exfiltrated data (if any) to determine notification obligations;
- Addressing customer concerns (*e.g.,* by providing identity monitoring services);
- Eliminating the vulnerability (*e.g.,* by enhancing security systems, conducting training, etc.); and
- Responding to regulator inquiries.

In addition, once the incident has been fully remediated, the company should review its incident response policies and procedures and address any deficiencies that it observed with regards to these procedures in practice.

5. LEGAL CONSIDERATIONS IN KEY JURISDICTIONS

While the mechanics of a ransomware attack and the technical prevention methods companies should employ remain the same across jurisdictions, different countries have different regulatory considerations that must be taken into account when responding to a ransomware attack.

Below we have provided some salient examples of these key jurisdiction-specific issues.

United States

Paying a ransom is not in and of itself a criminal offense under US law. However, payments to certain parties may violate US sanctions regimes. Specifically, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory in October 2020 cautioning companies that some ransomware attackers are sanctioned entities, and that therefore payment to these entities could be illegal. Parties that assist, sponsor, or provide financial, material, or technological support to these sanctioned parties may violate OFAC regulations and be subject to penalties on a strict liability basis—meaning that even if a party had no knowledge that it was engaging in a transaction with a sanctioned person or entity, penalties may apply. FINCEN also issued guidance reminding financial institutions of SAR-filing requirements arising from processing ransomware payments.

In addition, US breach notification laws create a significant compliance burden because they are state-specific. Therefore, typically a company's notification obligations will depend, in part, on the state of residence of any individuals whose personal data is compromised during the course of an attack. Thus, if personal data is exfiltrated during a ransomware attack, a time-consuming review of that data may be necessary to determine what notification obligations exist.

United Kingdom

Much as in the United States, there is no blanket ban on ransom payments in the United Kingdom, although companies should remain wary of counter-terrorism, anti-money laundering and sanction provisions. For instance, under s15(3) and s17 of the Terrorism Act 2000, a party will be liable for a ransomware payment if they knew or had reasonable cause to suspect that the funds would or may be used for the purposes of terrorism. Given the anonymous nature of most cyber-attackers, it is unlikely, although not impossible, that the payer will be liable under this law. Under anti-money laundering legislation, it is an offense to enter into in an arrangement which the party knows or suspect facilitates the use or control of criminal property (s328 of the Proceeds of Crime Act 2002). However, the courts have deemed that so long as funds are "clean" prior to the payment, this offense will not bite. Parties should also be wary of the risk surrounding financial sanctions as making payments, whether directly or indirectly, to "designate" individuals or entities listed in the consolidated list of financial sanctions targets prepared by OFSI is a criminal offense in the United Kingdom.

If you have already made a ransom payment, a recent High Court judgment suggests that courts are willing to help you recover that payment. In AA *period (v.)* Persons Unknown, the judge granted a proprietary injunction over a Bitcoin payment made following a cyber-attack to recover the funds from a cryptoasset exchange which housed the receiving account. The extent to which the courts and authorities in other jurisdictions are prepared to adopt an active role in ransomware cases remains to be seen.

Companies should also remain alert to the fact that notification obligations often create a much more pressing risk following a ransomware attack. Under Article 33 of the GDPR, organizations must report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach unless the breach is unlikely to result in a risk to individuals' rights and freedoms. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, organizations must also inform those individuals without undue delay. Further, the ICO has warned that businesses should have robust breach detection, investigation, and internal reporting procedures in place in order to facilitate decision-making about whether or not notifications are required. Although heavily reduced from the initially headlined amounts, the recent fines imposed on Marriott International and British Airways underscore the importance of deploying adequate data security measures and the value of cooperating with local regulators following any incident.

Germany

As in the United States, paying a ransom is not in and of itself a criminal offense in Germany. However, the US sanctions regime may also apply to German companies and therefore the considerations summarized above should be taken into consideration on a case-by-case basis.

Cyber-attacks usually trigger various notification requirements. In Germany, notification under Article 33 of the GDPR should generally be made to the data protection authority of the federal state where a company has its registered headquarters. In addition, data subjects need to be informed without undue delay if it is likely that the data breach resulted in a high risk to the rights and freedoms of natural persons (Article 34 GDPR). Further notification requirements may result from contracts between the affected company and its customers or under capital markets law.

Involvement of law enforcement authorities is usually not mandatory. However, law enforcement assistance may be beneficial in connection with potential negotiations with the attackers. Moreover, some cyber insurers may require that the police are informed.

Finally, certain companies, such as operators of critical infrastructure, cloud service providers, online marketplaces, and online search engines may fall under the IT Security Act which contains additional reporting requirements. In particular, such entities may have to inform the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI). Even in the absence of a legal obligation, informing the BSI should be considered as the BSI often has a good overview of ongoing attacks and can help identify the attackers or determine next steps.

France

The French National Cybersecurity Agency (ANSSI), together with the French Ministry of Justice (FMJ), published it September 2020 a guide on how to anticipate and react to ransomware attacks. Pursuant to this guide, when a company is subject to such an attack, the ANSSI and the FMJ (i) recommend not to pay the ransom and (ii) recommend to file a formal complaint (*plainte*) with the police (or *gendarmerie*) authorities. This complaint must be filed by the company that suffered the ransomware attack and may trigger the opening of an investigation that can lead to the identification of the attackers. This complaint is also often a prerequisite for the payment of damages (for instance, via insurance policies). In France, investigations relating to ransomware attacks and similar cyber-attacks are conducted by specialized units within the Paris prosecution service as well as within the police services.

In addition to the notification obligations that may be required under European laws and regulations (as encompassed, where relevant, by French law), in a case where the company suffering a ransomware attack is listed as an operator of "vital importance" (OVI) within the meaning of the French Defense Code, pursuant to the French law on critical infrastructure information protection, entered into effect on 20 December 2013, (as modified) this company must also notify the ANSSI if the ransomware attack occured on its critical information systems. This notification must include certain information, such as: a detailed explanation of the security incident; a detailed explanation of its consequences and corrective measures; and the technical details to enable the ANSSI to determine the level of risk (*e.g.,* whether the incident qualifies as a "major crisis").

Hong Kong

There is currently no law in Hong Kong prohibiting the payment of ransoms. While such payment could potentially be caught under section 25 of the Organized and Serious Crimes Ordinance (since the victim will have reasonable grounds to believe, or even know, that the ransom payment represents the attacker's proceeds of an indictable offense), section 25A provides a defense if the victim notifies an "authorized officer" (i.e. the Hong Kong police) of the payment in advance and obtains consent or if the victim notifies an authorized officer as soon as it is reasonable to do so after making the payment. In addition, victims should be mindful of the offenses under the United Nations Sanctions Ordinance (Cap. 537) and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526), in the unlikely event that a victim suspects or knows that the attacker is a sanctioned person, or is related to any act of production of weapons of mass destruction.

Although there is no cross-sector cybersecurity legislation in Hong Kong, industry-specific notification requirements may be relevant – for example, regulated financial institutions are expected to notify their regulators (the Securities and Futures Commission, the Hong Kong Monetary Authority, or the Insurance Authority) in the event of a major cyber incident. To the extent that personal data of customers is compromised, the Privacy Commissioner in Hong Kong also encourages companies to self-report and to notify the affected customers.

Singapore

While Singapore law does not specifically criminalize paying a ransom, this is actively discouraged by the Singapore authorities. Aside from there being no guarantee that the compromised files or systems can be recovered even if the ransom were to be paid, certain legislation may potentially be infringed depending on the circumstances.

For instance, payments to ransomware attackers may potentially infringe the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) which criminalizes assisting another person to retain, control, or use the benefits of criminal conduct. Similarly, ransom payments may potentially be caught by the Terrorism (Suppression of Financing) Act, which makes it an offense to provide property or services intending, knowing, or having reasonable grounds to believe that such property or services will be used to facilitate or carry out any terrorist act or to benefit any person facilitating or carrying out such activity. Payments to sanctioned entities may also violate Singapore sanctions laws.

In terms of notification obligations, the CDSA requires a report to be filed with the Commercial Affairs Department where there is knowledge or reasonable grounds to suspect that any property was used or is intended to be used in connection with criminal conduct. Where the ransomware attack affects critical information infrastructure or systems, the Cybersecurity Act and the Monetary Authority of Singapore require owners of such infrastructure or systems to file a report. In addition, where personal data has been compromised, and the scale of the personal data breach is significant and is likely to result in significant harm or impact to affected individuals, the Personal Data Protection Commission (PDPC) should be notified. Under amendments to the Personal Data Protection Act which are expected to come into force at the end of 2020, notification will be mandatory.

Australia

Ransom payments are not prohibited under Australian law but are actively discouraged by regulators. The Australian Cyber Security Centre (ACSC) advises against paying ransoms on the view that compromised organizations secure no guarantee that the damage will be reversed and further expose themselves to future attacks by doing so. There are similarly no mandatory reporting obligations or penalties for falling victim to cyber-attacks. Organizations may, however, seek to avail themselves of the ACSC's assistance in addressing any such cyber-attacks and in doing so, may adopt a prudent approach of reporting such cyber-attacks via the ACSC's ReportCyber portal.

The ACSC is the first port of call in reporting cyber-attacks. Reports made to the ACSC will not be considered formal police statements. However, all reports are utilized for assessment and intelligence initiatives by Australian law enforcement authorities and certain reports may be investigated in further detail.

Where there is an eligible data breach as part of a ransomware attack (in particular, where there has been exfiltration of data as part of the attack), there are specific requirements for organizations (if covered under the Privacy Act 1988 (Cth)) to notify the affected individuals and the Office of the Australian Information Commissioner (OAIC). An eligible data breach is assessed where there has been: (i) unauthorized access to or

disclosure of personal information held by a relevant organization; (ii) that inadvertent access or disclosure can be considered likely to cause serious harm to one or more individuals; and (iii) the organization is unable to mitigate that harm. If an eligible data breach has occurred, the relevant organization must notify the OIAC as soon as practicable as well as each affected individual.

6. HOW CC CAN HELP

The Clifford Chance privacy and cybersecurity team has extensive experience responding to ransomware and other types of cyber incidents both in the United States and globally.

Deep engagement with the changing regulatory landscape

We regularly assist multinational clients in navigating the complex global privacy and data protection landscape, including regulations such as the California Consumer Privacy Act, the fallout from the Schrems II decision and its impact on cross-border data transfers, the GDPR and NIS Directive, and the New York Department of Financial Service's Cyber Regulation.

A pragmatic, solution-focused approach

Our practice focuses on identifying solutions to our clients' problems, rather than answers to legal questions. We work with clients to assess risk and establish pragmatic approaches where certainty cannot be achieved. We adopt a market-tested, risk-based approach and strive to help clients prioritize and focus on key issues.

A highly experienced team

Our global team regularly advises clients on the full range of issues arising in the context of data privacy and cyber security. We have assisted multinational clients respond to dozens of cyber attacks, and are well versed in key jurisdictions' notification obligations and regulatory expectations. We have handled significant cyber attacks for clients, including a Fortune 100 consumer goods company, a multinational insurance conglomerate, and a global private equity fund. In addition, we have advised numerous clients, including major financial institutions, on their privacy and cyber security compliance obligations.

"Instead of just repeating the law, they give us a solution to our business challenges."

Data Protection & Information law: Chambers & Partners 2020

GLOBAL CYBERSECURITY CONTACTS

United States

Megan Gordon
Partner
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Daniel Silver
Partner
T: +1 212 878 4919
E: daniel.silver@cliffordchance.com

Ben Berringer
Associate
T: +1 212 878 3372
E: benjamin.berringer@cliffordchance.com

Brian Yin
Associate
T: +1 212 878 4980
E: brian.yin@cliffordchance.com

Paris

Dessislava Savova
Partner
T: +33 14405 5483
E: dessislava.savova@cliffordchance.com

Grégory Sroussi
Avocat
T: +33 14405 5248
E: gregory.sroussi@cliffordchance.com

Germany

Dr. Thomas Voland
Partner
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Ines Keitel
Partner
T: +49 697 199 1250
E: ines.keitel@cliffordchance.com

UK

Christian Vogel
Partner
T: +49 175 225 4859
E: christian.vogel@cliffordchance.com

Samantha Ward
Partner
T: +44 20 7006 8546
E: samantha.ward@cliffordchance.com

Kate Scott
Partner
T: +44 20 7006 4442
E: kate.scott@cliffordchance.com

Hong Kong

Donna Wacker
Partner
T: +852 2826 3478
E: donna.wacker@cliffordchance.com

William Wong
Consultant
T: +852 2826 3588
E: william.wong@cliffordchance.com

Singapore

Luke Grubb
Partner
T: +65 56 506 2780
E: luke.grubb@cliffordchance.com

Kabir Singh
Partner
T: +65 6410 2273
E: kabir.singh@cliffordchance.com

Australia

Tim Grave
Partner
T: +61 2 8922 8028
E: tim.grave@cliffordchance.com

Kirsten Scott
Counsel
T: +61 8 9262 5517
E: kirsten.scott@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2012-000794